

REMARKS

Claims 1-39 are pending in this application. By this amendment, Applicants have amended claims 1, 21, 25 and 39, canceled claims 37 and 38 and added claims 40 and 41. Reconsideration of the above-identified application in view of the foregoing amendments and the following remarks is respectfully requested.

Rejections Under 35 U.S.C. § 112, ¶1:

In the Office Action, claims 33 and 34 were rejected under 35 U.S.C. § 112, ¶1 as allegedly failing to comply with the enablement requirement.

Applicants respectfully submit that claim 33, is “open-ended” through its use of the term “comprising”, and thus, its recitation of “determining whether the service has been dropped; if the service has been dropped ...” does not preclude the client from receiving the encrypted service again prior to the performance of the remaining steps of claim 33 – namely, “determining whether either the first decryption information or the second decryption information is valid decryption information; if one of the first decryption information or the second decryption information is valid decryption information, decrypting the service with the valid decryption information.

For example, the service may have been dropped due to a temporary event, such as interference or the client’s having wandered outside of the coverage area. (See, e.g., p. 7, lines 17-20). In that case, nothing in claim 33 precludes the receipt of the encrypted service again after its having been dropped, and the client through the use of, e.g., synchronization information provided by the service provider or trial and error (p. 14, lines 21-23), trying to decrypt the service using the decryption information in its possession. In so doing, the client may determine whether the decryption information is valid and, if valid, the client may continue to decrypt the

service using the valid decryption information. However, if the decryption information is no longer valid given the passage of time between the encrypted service having been dropped and its having been received again, the client may, as set forth in claim 34, re-connect to, and authenticate with, the service provider, receive valid decryption information therefrom and decrypt the service using the valid decryption information.

Accordingly, Applicants respectfully submit that claims 33 and 34 comply with the enablement requirement of 35 U.S.C. § 112, ¶1 and request that the present rejections be withdrawn.

Rejections Under 35 U.S.C. §102(e):

In the Office Action, claims 1-7, 11, 14-19, 21-27, 30-32, 35, 36 and 39 were rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,516,412 to Wasilewski et al. (“Wasilewski”). Claims 1, 21, 25 and 39 are independent.

Applicants’ invention, as defined by amended claim 1, is directed to a method for a service provider to transmit decryption information in a secure manner, comprising: receiving a request for a service from a requestor over a bi-directional channel; authenticating the requestor; transmitting first decryption information to the requestor over the bi-directional channel, wherein the first decryption information decrypts the service; transmitting the service, encrypted with encryption information corresponding to the first decryption information, over a unidirectional channel; generating second decryption information for use in decrypting the service; transmitting the second decryption information over the unidirectional channel; and transmitting the service, encrypted with encryption information corresponding to the second decryption information, over the unidirectional channel.

Wasilewski is directed to a conditional access system wherein a program, such as an MPEG-2 program, is encrypted with a code word and broadcast to a set-top box. The code word, encrypted using a multi-session key (MSK), is included in the broadcast in an Entitlement Control Message (ECM). The MSK is sent to the set-top box in encrypted form, in one embodiment, in an Entitlement Management Message (EMM) that is sent as part of the broadcast or, in an alternate embodiment, in the EMM sent over another channel. A user also may submit a forward purchase message (FPM) to subscribe to a program. Upon receipt of the encrypted program, the set-top box uses a private key and an associated public serial number to decrypt the MSK, which, in turn is used to generate the codeword. The set-top box then uses the code word to decrypt the program. (See, generally, Wasilewski, Figs. 1, 2A, 2B, 3 and 4)

The Office Action equates the multi session key (MSK) and the code word (CW) of Wasilewski with the “first decryption information ... [transmitted] over the bi-directional channel” and the “second decryption information [transmitted] over the unidirectional channel”, respectively, of claim 1. (See Office Action, p. 4) Claim 1, as amended, however, requires that “the first decryption information decrypts the service”. In contrast, in Wasilewski, it is the code word, which the Office Action equates with the second decryption information, that decrypts the MPEG-2 program. (See, e.g., Wasilewski, Fig. 2B, reference numeral 238) The MSK of Wasilewski, which the Office Action equates with the first decryption information, simply decrypts the code word, rather than the MPEG-2 program. (See, e.g., Fig. 2B, numeral 236) Accordingly, claim 1 is not anticipated by Wasilewski for this reason alone.

However, claim 1 further requires “transmitting the service encrypted with encryption information corresponding to the first decryption information”. In contrast, Wasilewski transmits the MPEG-2 program encrypted with the code word (See, e.g.,

Wasilewski, Fig. 2A, reference numerals 201, 202), which the Office Action equates with the “second decryption information”, rather than with the MSK, which the Office Action equates with the “first decryption information”. Thus, Wasilewski does not transmit the MPEG-2 program encrypted with encryption information corresponding to the first decryption information, as required by claim 1. Accordingly, amended claim 1 is not anticipated by Wasilewski for this additional reason.

Claims 21, 25 and 39, as amended, contain features similar to those found in amended claim 1, and thus, are allowable for at least the same reasons as set forth above in urging the allowance of amended claim 1. In addition, with respect to claim 39, the code word of Wasilewski is not “installed ... on a device of the requestor”, as required by claim 39, but instead is generated by the set-top box (see, e.g., Fig. 1, reference numeral 119), and thus, claim 39 is not anticipated by Wasilewski for this additional reason.

Dependent Claims:

Applicants do not believe it necessary at this time to address the rejections of the dependent claims as Applicants believe that the foregoing places the independent claims in condition for allowance. Applicants, however, reserve the right to address those rejections in the future should such a response be deemed necessary and appropriate.

New Claims:

Applicants have added new claims 40 and 41, which are believed to be patentable over Wasilewski for reasons similar to those set forth above in urging the allowance of amended claim 1.

CONCLUSION

Applicants respectfully submit that this Application is in condition for allowance for which action is earnestly solicited.

If a telephone conference would facilitate prosecution of this Application in any way, the Examiner is invited to contact the undersigned at the number provided.

AUTHORIZATION

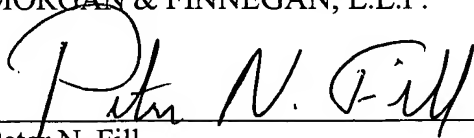
The Commissioner is hereby authorized to charge any additional fees which may be required by this response, or credit any overpayment to Deposit Account No. 13-4500, Order No. 4208-4027. A DUPLICATE COPY OF THIS PAPER IS ATTACHED.

In the event that an extension of time is required, or which may be required in addition to that requested in a petition for an extension of time, the Commissioner is requested to grant a petition for that extension of time which is required to make this response timely and is hereby authorized to charge any fee for such an extension of time or credit any overpayment for an extension of time to Deposit Account No. 13-4500, Order No. 4208-4027. A DUPLICATE COPY OF THIS PAPER IS ATTACHED.

Respectfully submitted,
MORGAN & FINNEGAN, L.L.P.

Dated: April 10, 2006

By: _____


Peter N. Fill
Registration No. 38,876

Correspondence Address:

MORGAN & FINNEGAN, L.L.P.
3 World Financial Center
New York, NY 10281-2101
(212) 415-8700 Telephone
(212) 415-8701 Facsimile